ABSTRACT

Each connection can have a different symmetric key derived from a previously exchanged master secret in a symmetric key cryptography scheme. In one embodiment, the invention includes establishing a master secret between the first communications device and a second communications device, perhaps during registration. Then a connection is opened between the first communications device and the second communications device. A connection secret is generated from the master secret, and using as a symmetric key during the life of the connection.